$$
\begin{tikzcd}
A \arrow[r, "\phi\quad\psi"] \arrow[d] & B \arrow[d, "\xi"] \\
C \arrow[r, "\eta"] & D
\end{tikzcd}
$$

$\mathcal{ABCDEFGHIJKLNMOPQRSTUVWXYZ}$
$\mathit{abcdefghijklnmopqrstuvwxyz}$
$\mathfrak{ABCDEFGHIJKLNMOPQRSTUVWXYZ}$
$\mathfrak{abcdefghijklnmopqrstuvwxyz}$
$\boldsymbol{ABCDEFGHIJKLNMOPQRSTUVWXYZ}$
$\boldsymbol{abcdefghijklnmopqrstuvwxyz}$
$\rightarrow\rightarrowtail\twoheadrightarrow$

Part I

Grundlagen

iUnterobjekte und Quotientenobjekte

Sei $\boldsymbol{A}$ eine Kategorie. Dann definieren wir den Verband der Unterobjekte $\operatorname{Sub} A$ für jedes Objekt $A : \boldsymbol{A}$ als die Isomorphieklassen der Kategorie $\rightarrowtail_{\boldsymbol{A}} A$ (also $\rightarrowtail_{\boldsymbol{A}} A/\leftrightarrow$). Analog definieren wir den Verband der Quotienten von A als $\operatorname{Quot} A$ durch die Isomorphieklassen von $A \twoheadrightarrow_{\boldsymbol{A}} / \leftrightarrow$. Die beiden Konzepte sind also genau dual zueinander.

iiKerne und Kokerne

Sei $\phi : A \rightarrow_{\boldsymbol{A}} B$ ein Morphismus. Dann wird die Isomorhpieklasse $\ker\phi$

$$
\begin{tikzcd}
\ker\phi \arrow[r] & A \arrow[r, "\phi"] & B \\
C \arrow[u, "\exists_1"] \arrow[ur, "0"'] \arrow[urr] & &
\end{tikzcd}
$$

Satz 0.1. *Sei $\phi : A \rightarrow B$ ein Morphismus. Dann sagen wir ϕ genügt dem ersten Isomorphiesatz, falls Isomorphieklassen* $\operatorname{im}\phi$ *und* $\iota : \operatorname{im}\phi \rightarrowtail B$ *gibt, sodass* $\phi = \pi\iota$

iiiProdukte und Koprodukte

Sei $\boldsymbol{B} \rightarrowtail \boldsymbol{A}$ eine Unterkategorie.

ivGruppenaxiome

Unter einer Gruppe verstehen wir eine Struktur vom Typ $\boldsymbol{Grp} = \left\langle \circ, ^{-1}, 1 \right\rangle$, derart dass folgende Identitäten gelten

- $(a \circ b) \circ c = a \circ (b \circ c)$ (Assoziativität)
- $a^{-1} \circ a = a \circ a^{-1} = 1$ (Inversenabblildung)
- $a \circ 1 = 1 \circ a = a$ (neutrales Element)

Satz 0.2. *Hallo*

vDie Sylow'schnen Sätze

Eine natürliche Frage, welche sich aus dem Theorem von Lagrange ergibt, welche Aussagen über die Anzahl und Art der Untergruppen von Ordnung n einer endlichen Gruppe G getroffen werden können. Für $n \nmid |G|$ ist selbige Anzahl nach dem Theorem von Lagrange (TODO: REF) gleich null. Ist G zyklisch, so ist jene Anzahl im Falle $n|\,|G|$ genau eins. Tatsächlich muss es aber für $n|\,|G|$ keine Untergruppen dieser Ordnung geben, was man am leichtesten an der symmetrischen Gruppe $\operatorname{Aut} m$ sieht, denn wählt man nun n als eine Zyklizität erzwingende Zahl, sodass $m < n|m!$, dann gibt es offensichtlich keine Untergruppen von $\operatorname{Aut} m$ dieser Ordnung. ist es ob bei einer endlichen Gruppe G der

Tatsächlich lassen sich aber befriedigende Aussagen treffen, falls $n = p^e$ die Potenz einer Primzahl p ist. Diese werden gemeinhin als Sylow'sche Sätze bezeichnet.

Definition 0.1 (p-Gruppe). Sei G eine Gruppe derart, dass jedes Element $g \in G$ eine Primzahlpotenz p^{e_g} als Ordnung hat (wobei p eine feste Primzahl sei.

Bemerkung 1. Eine triviale Konsequenz der Sylow'schen Theoreme wird es sein, dass jede endliche p-Gruppe selbst von Primzahlpotenzordnung p^e ist.

Satz 0.3 (Existenz von p-Untergruppen jeder Ordnung). *Sei G eine endliche Gruppe mit $|G| = p^e n$. Für die Anzahl $N_{p^e} := |\{U \leq G : |U| = p^e\}|$ gilt dann*

$$N_{p^e} = 1 \; mod \; p$$

Beweis. Wir betrachten die Aktion von G auf den p^e-elementigen Untermengen von $G_{\boldsymbol{Set}}$ welche gegeben wird durch elementweise Rechtsmultiplikation. Die Bahnengleichung für diese Aktion wird dann zu

$$\left|\binom{G_{\boldsymbol{Set}}}{p^e}\right| = \sum_i \left|G/\mathrm{stab} A_i\right|,$$

wobei A_i Repräsentanten der G-Bahnen sind. Für $A_i \rightarrowtail G_{\boldsymbol{Set}}$, $|A_i| = p^e$ gilt allerdings dann $A_i(\mathrm{stab} A_i)_{\boldsymbol{Set}} = A_i$, also ist A_i eine disjunkte Vereinigung von

Linksnebenklassen von $\mathrm{stab} A_i$ und mithin $|\mathrm{stab} A_i| \,|p^e$. Betrachten wir also obige gleichung modulo pn, so folgt

$$\binom{p^e n}{p^e} = nN_{p^e} \mod pn,$$

denn alle Terme, in denen $\mathrm{stab} A_i < p^e$ ist in obiger Gleichung entfallen und die übrigen Terme zählen genau für jede p^e-elementige Untergruppe von G ihre Linksnebenklassen (derer gibt es n). Daraus folgt

$$\frac{1}{n}\binom{p^e n}{p^e} = \binom{p^e n - 1}{p^e - 1} = N_{p^e} \mod p,$$

wobei der Ausdruck auf der Linken Seite gleich 1 ist modulo p. Dies sieht man einerseits daran, dass dies für die zyklische Gruppe mit $p^e n$ Elementen gilt, andererseits lässt sich auch das Theorem von Lucas (TODO : REF) auf den letzten Binomialkoeffizienten anwenden. Wir erhalten dann

$$N_{p^e} = \binom{p^e n - 1}{p^e - 1} = \binom{p-1}{p-1}^e = 1 \mod p.$$

■

Text

Satz 0.4. *Jede endliche Gruppe G hat p-Sylow-Gruppen. Für jede p-Untergruppe U und eine p-Sylow-Gruppe von G gibt es ein Element $g \in G$, sodass $U \rightarrowtail P^g$. Insbesondere sind alle p-Sylow-Gruppen konjugiert zueinander und ihre Anzahl ist $|G/N_G P|$.*

viDie Sätze von Hall

Die Sätze von Hall stellen eine Verallgemeinerung der Sylow'schen Sätze für auflösbare Gruppen dar.

Satz 0.5 (Hall'sches Theorem). *Sei G auflösbar und $|G| = mn$ mit teilerfremden m und n. Dann gilt*

(I) Sei U eine Untergruppe mit $|U|\,|m$ und M eine Untergruppe der Ordnung m, dann gibt es ein $g \in G$ sodass $U \leq M^g$.

(II) Für die Anzahl der Untergruppen der Ordnung m von G gilt:

$$N_m = 1 \; mod \; \mathrm{rad} m$$

Beweis. Der Beweis erfolgt per Induktion nach der Anzahl k der Primfaktoren von m. Für $k = 1$ gilt die Aussage schlicht aufgrund der Sylow'schen Sätze auch ohne Auflösbarkeit von G. ■

Satz 0.6 (FRATTINI-Argument). *Sie G eine Gruppe und $N \leq_{\mathrm{Con}\, G} G$. Weiter sei P eine Untergruppe von N derart, dass alle zu P isomorphen Untergruppen in H konjugiert sind (also z.B. P eine p-SYLOW-Gruppe). Dann gilt $G = \mathrm{N}_G PN$.*

Beweis. Für $g \in G$ ist P^g isomorph zu P und gleichermaßen Untergruppe von N, da N normal in G liegt. Also sind P und P^g in N konjugiert und es folgt $P^{g^n} = P$ für geignetes $n \in N$. Damit ist aber $gn \in \mathrm{N}_G P$ und somit auch $g \in N\mathrm{N}_G P$. ∎

viiAuflösbarkeit von Gruppen

Definition 0.2 (Subnormalenverband, Subnormalenreihe). Ein Unterverband $\boldsymbol{U}$ von $\mathrm{Sub}\, G$ Subnormalenverband, falls für alle $U \in \boldsymbol{U}$ gilt $U \in \mathrm{Con} \bigwedge_{V>U} V$. Ist ein solcher Verband isomorph zu einem Unterverband von $\mathbb{N}_{\boldsymbol{Lat}}$, so nennen wir Ihn eine Subnormalenreihe.

Definition 0.3 (Auflösbare Gruppe). Eine Gruppe G heißt *auflösbar*, falls es einen Subnormalenverband von G gibt, derart, dass

$$\bigwedge_{V>U} V/U \text{ kommutativ}$$

für alle $U \in U$. *endlich auflösbar*[1]

Definition 0.4 (Kommutatoruntergruppe). Seien $A, B \in \mathrm{Sub}\, G$. Dann bezeichnen wir mit $\langle [A_{\boldsymbol{Set}}, B_{\boldsymbol{Set}}] \rangle_{\mathrm{Sub}\, G}$ die *Kommutatoruntergruppe* von A und B.

Lemma 0.1. *Die Kommutatoruntergruppe zweier Untergruppen A und B zeichnet sich durch folgende universelle Eigenschaft aus. $\langle [A_{\boldsymbol{Set}}, B_{\boldsymbol{Set}}] \rangle_{\mathrm{Sub}\, G} \in \mathrm{Con}\, A \vee B$.*

Beweis.

∎

Definition 0.5 (Kommutatorreihe). Wir definieren die *Kommutatorreihe* $\left(G^{(i)}\right)_{i \in \mathbb{N}}$ einer Gruppe G als

$$G^{(0)} := G,\ G^{(i+1)} := \left\langle \left[G^{(i)}_{\boldsymbol{Set}}, G^{(i)}{}_{\boldsymbol{Set}} \right] \right\rangle_{\mathrm{Sub}\, G} \quad (i \in \mathbb{N}).$$

Weiterhin setzen wir $G^{(\omega)} := \bigwedge_{i \in \mathbb{N}} G^{(i)}$ und bezeichnen es als *perfekten Kern* von G.

Lemma 0.2. *Eine Gruppe G ist genau dann endlich auflösbar, falls ihre Kommutatorreihe nach endlich vielen Schritten in 1 endet. Sie ist genau dann ω-auflösbar, falls ihr perfekter Kern gleich 1 ist.*

Beweis. Sei $\boldsymbol{G}$ ∎

[1] Dies meint auflösbar im herkömmlichen Sinne.

vii.1 Der Satz von Jordan-Hölder

viiiNilpotenz von Gruppen

Im folgenden betrachten wir eine Eigenschaft von Gruppen die mit *Nilpotenz* bezeichnet wird. Sie stellt in gewissem Sinne eine Verallgemeinerung der Eigenschaft einer Gruppe dar, kommutativ zu sein.

Definition 0.6 (Invariantenfilter). Ein *Invariantensystem* einer Gruppe G ist ein Unterverband von $\operatorname{Con} G$. Eine *Invariantenreihe* ist eine zu $\mathbb{N}$ isomorphes Invariantensystem.

Definition 0.7 (Zentralreihe). Eine Invariantenreihe $(C_i)_{i\in\mathbb{N}}$ heißt *Zentralreihe*, wenn G_i/G_{i+1} im Zentrum von G/G_{i+1} liegt.

$$\bigwedge$$

Definition 0.8 (Untere Zentralreihe γ_i). Die *untere Zentralreihe* $(\gamma_i G)_{i\in\mathbb{N}}$ ist definiert als

$$\gamma_0 G = G,\ \gamma_{i+1}G = [G, \gamma_i G]\ (i \in \mathbb{N})$$

und insbesondere ist $(\gamma_i)_{i\in I}$ wirklich eine Zentralreihe.

Lemma 0.3 (charakterisierende Eigenschaft der unteren Zentralreihe). *Sei $(C_i)_{i\in\mathbb{N}}$ eine antitone Zentralreihe einer Gruppe G, dann gilt $\gamma_i G \leq C_i$ ($i \geq 0$).*

Beweis. Mit Induktion nach i. Für $i = 0$ haben wir $\gamma_0 G = G = C_0$. Für $i \in \mathbb{N}$ gilt weiterhin $\gamma_{i+1}G = [G, \gamma_i G] \leq [G, C_i] \leq C_{i+1}$ (da $C_i/C_{i+1} \leq Z(G/C_{i+1})$). Damit ist die Induktion abgeschlossen und es verbleibt die Zentralreiheneigenschaft von $(\gamma_i G)_{i\in I}$ nachzuweisen. Diese ist jedoch leicht zu überprüfen durch $\gamma_{i+1} = [G, \gamma_i G] \leq \gamma_{i+1}$, also liegt $\gamma_i G/\gamma_{i+1}G$ im Zentrum von $G/\gamma_{i+1}G$. ■

Definition 0.9. Die *obere Zentralreihe* $(Z_i G)_{i\in\mathbb{N}}$ ist definiert durch

$$Z_0 G = 1,\ Z_{i+1}G/Z_i G = Z(G/Z_i)\ (i \in \mathbb{N}).$$

Lemma 0.4 (charakterisierende Eigenschaft der oberen Zentralreihe). *Sei $(C_i)_{i\in\mathbb{N}}$ eine monotone Zentralreihe, dann gilt*

$$G_i \leq Z_i G$$

und insbesondere ist $(Z_i G)_{i\in\mathbb{N}}$ wirklich eine Zentralreihe.

Beweis. Mit Induktion nach i. Für $i = 0$ gilt $Z_0 G = G = C_0$. Für $i \in \mathbb{N}$ gilt weiterhin $C_{i+1}/C_i \leq Z(G/C_i)$, was gleichbedeutend ist mit $[C_{i+1}, G] \leq C_i$.

Damit gilt aber $[C_{i+1}, G] \leq Z_i G$ womit andererseits folgt, dass $C_{i+1} \leq Z_{i+1}G$. Damit ist die Induktion abgeschlossen und es verbleibt die Zentralreiheneigenschaft von $(Z_i G)_{i \in I}$ nachzuweisen. Diese folgt aber nach Definition trivial, denn $Z_{i+1}G/Z_i G = Z(G/Z_i) \leq Z(G/Z_i)$. ∎

Definition 0.10 (Nilpotenz). Eine Gruppe G heißt *nilpotent*, falls es eine monotone Zentralreihe gibt, die gegen G konvergiert und *nilpotent*, falls es eine antitone Zentralreihe gibt, die gegen 1 konvergiert.

Satz 0.7 (Charakterisierung von Nilpotenz). *Die folgenden Aussagen sind für eine endliche Gruppe G äquivalent.*

(I) G ist nilpotent.

(II) Die untere Zentralreihe endet mit der trivialen Gruppe: $\exists n \in \mathbb{N} : \gamma_n G = 1$.

(III) Die obere Zentralreihe von G endet mit G: $\exists n \in \mathbb{N} : Z_n G = G$.

(IV) Für $U \in \operatorname{Sub} G$, $U \neq G$ gilt $U < N_G U$.

(V) Für $U \in \operatorname{Sub} G$, $U \neq 1$ gilt $[G, U] < U$.

(VI) Jede maximale Untergruppe von G ist normal in G.

(VII) G ist das direkte Produkt seine p-Sylow-Gruppe.

(VIII) Je zwei Elemente von koprimer Ordnung kommutieren.

Beweis.

(I) Sei P eine maximale p-Untergruppe, dann folgt aus $\mathrm{N}_G P < G$, dass $\mathrm{N}_G^2 P = \mathrm{N}_G P$. Also ist G nicht nilpotent.

∎

ixMinimale Normalteiler und charakteristisch einfache Gruppen

Lemma 0.5 (Zusammenspiel zwischen normal und charakteristisch). *Sei C charakteristisch in N und N normal in G. Dann ist N normal in G.*

Beweis. Jede Konjugation (innere Automorphismus) in G lässt C fix, beschränkt sich also zu einem Automorphismus von N. Damit lässt sie auch C fest, nach Definition von charakteristisch. ∎

Lemma 0.6. *Sei N ein minimaler Normalteiler einer Gruppe G. Dann ist N charakteristisch einfach.*

Beweis. Sei $1 < C$ eine charakteristische Untergruppe von N. Dann ist nach Lemma 0.5arabic6 auch C normal in G. Nach Minimalität von N folgt $N \leq C$ somit also $N = C$. Also ist N charakteristisch einfach. ∎

Satz 0.8 (Charakterisierung charakteristisch einfacher Gruppen). *Eine Gruppe G mit minimalem Normalteiler N ist genau dann charakteristisch einfach, falls N einfach ist und sie eine Potenz von N ist.*

Beweis. Sei G charakteristisch einfach und N minimaler Normalteiler. Die Bilder von N unter $\operatorname{Aut} G$ erzeugen eine nicht-triviale charakteristische Untergruppe von G, also ganz G. Sind weiter N und M zwei solcher Bilder, dann gilt $N = M$ oder $N \wedge M = 1$, da $N \wedge M \leq N$ ein Normalteiler von G ist. Also folgt für verschiedene N und M, dass $\langle [M_{\mathbf{Set}}, N_{\mathbf{Set}}] \rangle_{\operatorname{Sub} G} \leq M \wedge N = 1$, somit M und N elementweise kommutieren. Damit ist G das Produkt all jener Bilder, da diese — wie schon erwähnt — G erzeugen. Weiter muss dann N einfach sein, da jeder Normalteiler L von N aufgrund der Produktdarstellung von G, dann auch normal in G liegt.

Für die Rückrichtung nehmen wir an, dass $G = \prod S_i$. ∎